Setting Up Public Key Authentication

Category: Security & Logging In

Follow the steps below to set up your public key authentication.

Step 1: Create an SSH Public/Private Key Pair

To use public key authentication with the Secure Front Ends (SFEs), you need to have an SSH public/private key pair. If you do not, you can create a SSH public/private key pair by typing the following command and following the prompts:

```
your_localhost% ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/username/.ssh/id_rsa): ENTER
Enter passphrase (empty for no passphrase):enter a passphrase of your choice
Enter same passphrase again: type your passphrase again
Your identification has been saved in /Users/username/.ssh/id_rsa.
Your public key has been saved in /Users/username/.ssh/id_rsa.pub.
```

Your passphrase for the private key must meet NASA password requirements.

If you are using a non-Unix system, please consult your SSH documentation.

Step 2: Copy SSH Public Key to SFEs

Copy the public key file to your **~/.ssh2** directory on the SFEs (for example, sfe*1*):

```
your_localhost% scp ~/.ssh/id_rsa.pub
username@sfe1.nas.nasa.gov:.ssh2
```

On the SFEs, type the following command:

```
sfe1% echo "Key id_rsa.pub" > .ssh2/authorization
```

NOTE: Use only one space between the word "Key" and the public key filename.

To test your public/private key pair, type the following command on your localhost:

```
your_localhost% ssh -i ~/.ssh/id_rsa username@sfe1.nas.nasa.gov
```

You will be prompted for both your SecurID passcode and your private key passphrase.

TIP: Setting up public key authentication for sfe[*1-4*] gives you the freedom of using any of the four secure front ends.

Article ID: 230
Last updated: 14 Sep, 2012
The HEC Environment -> Security & Logging In -> Setting Up Public Key Authentication
http://www.nas.nasa.gov/hecc/support/kb/entry/230/?ajax=1